SprintSecure^{sm} Web Protection
Product Annex

The following terms and conditions in this **SprintSecure**^{sm} Web Protection Product Annex ("Annex"), together with the Sprint Standard Terms and Conditions for Communications Services ("Standard Terms and Conditions") and the agreement ("Agreement") under which Customer is purchasing SprintSecure Web Protection, govern Sprint's provision of SprintSecure Web Protection to Customer. Terms not otherwise defined herein will have the meanings set forth in the Standard Terms and Conditions and the Agreement.

1. SERVICE COMPONENTS.

1.1. Eligibility. SprintSecure Web Protection services are only available to customers of Sprint's Dedicated Internet Access and Global MPLS products. If Customer attempts to order SprintSecure Web Protection services, but does not have Sprint's Dedicated Internet Access and Global MPLS products, Customer's order will be rejected.

1.2. Web and IM Security Services. Sprint's Web and IM security services ('the Services') are comprised of Web Malware Scanning, Web Filtering and Instant Messaging Control as described below. The Customer's external HTTP, HTTPS and FTP over HTTP requests (including all attachments, macros or executables) are directed through the Services. The configuration settings required to direct this external traffic via the Services are made and maintained by the Customer (with assistance and support from Sprint as reasonably required) and depend on the Customer's technical infrastructure. The Customer must ensure that internal HTTP/HTTPS/FTP over HTTP traffic (e.g. to the corporate intranet) is not directed via the Services.

A. Web Malware Scanning ("MS")

(1) Once the relevant configuration changes are made, unencrypted Web pages and attachments will be scanned by Outbreak IntelligenceTM, a proprietary security platform that detects malware threats by using a combination of multiple, correlated detection technologies, including industry leading anti-malware engines.

(2) MS will scan as much of the Web page and its attachments as possible. It may not be possible to scan certain Web pages or attachments (for example, password protected). Unscannable attachments will be blocked. Encrypted traffic (i.e. HTTPS/SSL) cannot be scanned and will be passed through MS unscanned.

(3) If a Customer's Web page or attachments are found to contain malware (or deemed unscannable in accordance with Section 1.2.A(2), except for SSL traffic), then access to that Web page or attachment is denied and the Internet user will be displayed an automatic alert Web page. Notification may also be sent by email to a Customer administrator.

B. Web Filtering ("WF")

(1) Once the relevant configuration changes are made, Web pages and attachments will be filtered using industry leading URL categorization and content analysis. URLs are categorized by reference to a number of predefined categories as specified in ScanCenter (see Section 1.4).

(2) The Customer is able to configure WF to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet users or groups. A number of additional features (for example, 'blocked' and 'allowed' list functionality) are also available.

(3) WF will filter as much of the Web page and its attachments as possible. It may not be possible to filter certain Web pages or attachments (for example, password protected). Customers may also configure specific exceptions for web sites that should not be filtered. Encrypted traffic (i.e. HTTPS/SSL) cannot be filtered and will be passed through WF unless otherwise specified by the Customer in relation to specific categories of content. WF will only filter Web pages that are categorized by WF in accordance with the category that the Customer has chosen to filter.

(4) The Customer has the option of performing individual and/or group administration and reporting capabilities by utilizing the Connector software described in Section 1.3.

(5) If an Internet user requests a Web page or attachment where an access restriction policy applies, then access to that Web page or attachment is denied and the user will be displayed an automatic alert Web page. Notification may also be sent by email to a Customer administrator.

C. Instant Message Control ("IMC")

(1) The Customer's external Instant Message requests as prescribed by Sprint (currently those used by Windows Live / .NET Messenger Service, Yahoo! Messenger, AOL Instant Messenger and Jabber/Google Talk), including all

macros, messages or executables, are directed through the Service. The configuration settings required to direct this external traffic via the Service are made and maintained by the Customer and depend on the Customer's technical infrastructure. Sprint Technical Support will advise the Customer on making these changes if required.

(2) Once the relevant configuration changes are made, Instant Messages will be scanned by industry leading anti-malware and Instant Message spam analysis systems, including Outbreak IntelligenceTM.

(3) The Customer is able to configure IMC to create access restriction policies (based both on categories and types of content) and deploy these at specific times to specific Internet users or groups. A number of additional features (for example, 'blocked' and 'allowed' list functionality, Instant Message protocol allowing/disabling) are also available.

(4) IMC will scan as much of the Instant Message as possible. It may not be possible to scan certain Instant Messages (for example, password protected). Unscannable messages will be blocked. Encrypted traffic cannot be scanned and will be passed through IMC unscanned. IMC will only filter Instant Message content in accordance with the dictionaries that the Customer has chosen to filter.

(5) If an Internet user sends or receives Instant Message content for which an access restriction policy applies, then access to that Instant Message is denied and the user will be displayed an automatic alert event. Notification may also be sent by email to a Customer administrator.

(6) If an Instant Message is found to contain malware (or deemed unscannable), then that Instant Message will not be transmitted, and the end user will be displayed an Instant Message alert message. Notification may also be sent by email to a Customer administrator. IMC will display notification messages concerning monitoring of Instant Messages as stipulated by the Customer.

(7) IMC will monitor and log Instant Message messages, and output this information to a third party archiving system, as well as make this information available through ScanCenter for the standard data retention period.

(8) IMC will display notification messages concerning monitoring of Instant Messages as stipulated by the customer.

1.3. Connector.

(A) Sprint will make available optional software ("Connector") to Customers. If ordered by the Customer, Sprint will provide the Connector software to the Customer for the Customer to install in their network in accordance with Sprint installation guidelines.

(B) The Connector enables users to connect to the Services even without a static IP address by using an authentication key. If users have other services that rely on a fixed IP address for identification, they can configure direct connections for specific websites, domains, hosts or networks. Administrators can create, revoke, activate, and deactivate authentication keys for connectors per group or per users.

(C) The Connector does not support all potential Customer systems and set-ups.

1.4. Customer Interface.

(A) Customer will be provided access to a Web-based portal, hosted by Sprint, to administer and report on the Services.

(B) Access to ScanCenter is via a secure (https) website and is password-protected.

(C) Customers can have multiple administrators for a single account. Customers can give each administrator a unique login and provide full access or read only privileges specific to each user. This functionality allows a unique, single Super User account that can create multiple administrators.

(D) ScanCenter enables the Customer administrator to:

(1) review statistics of all malware stopped and Web content blocked;

(2) create access restrictions and apply these to specific users or groups (if the Connector has been installed by the Customer in accordance with this Annex);

(3) customize browser alert pages seen by users when web access to a particular site or file is denied;

(4) update administration details for real-time email alerts; and

(5) configure and schedule automated system auditing and reporting.

(E) Automated reports are available on overall traffic, bandwidth, blocked URLs and malware stopped. ScanCenter also offers a comprehensive selection of additional reports, generated daily, which provide in-depth analysis in the form of graphs, tables, and exportable data files. Customer can schedule regular reports for different service functionality and specify users, times, and email it to certain users or groups.

(F) Audit Logging functionality records administration, configuration, filtering, and policy changes made for the Customer's Services, and can be configured by full access administrators or the Super User. Auditing includes who made the change, what was changed, and when it was changed. Audit logs can be searched by specifying a time period, category or type of logs, and type of action taken.

(G) Privacy Logging functionality, when enabled, will log when web pages are blocked according to web filtering policy, but will obfuscate private details such as source username and IP address. This feature is for Customers who must comply with local privacy policies or regulations.

1.5. Block Alert Pages.

(A) Block alert pages are dynamically generated HTML pages displayed to end users when they are prevented from accessing prohibited Web content. Customer can choose a standard block alert page or their own customized content which can be uploaded via ScanCenter (see Section 1.3). Sprint will host the Blocked pages. A user guide is available to Customers.

2. PARTIES' RESPONSIBILITIES.

2.1. Customer's Responsibilities.

(A) Customer will provide Sprint with all technical data and all other information Sprint may reasonably request from time to time to allow Sprint to supply the Services to Customer. The Services do not include Customer's access connection to the Internet or any equipment necessary for Customer to make such connection, which are Customer's sole responsibility.

(B) Customer recognizes that information sent to and from Customer will pass through Sprint systems and accordingly Customer agrees that it must:

(1) comply with all relevant legislation applicable to Customer's use of the Internet;

(2) not use the Internet for any unlawful purpose; and

(3) indemnify Sprint against any liability to third parties resulting from information passing through Sprint systems to or from Customer.

(C) Customer is solely responsible for its activities in using the Services including the activities of its employees and contractors and all parties that it allows to have access to the Services.

(D) Customer must comply with the Web and Email Security Services – Acceptable Use Policy attached to this Annex as Exhibit 1 and as it may be amended from time-to-time.

2.2. Sprint Responsibilities.

(A) Sprint will send Customer a service provisioning email that will explain the necessary technical changes Customer will need to make to use the Services. If the Connector has been ordered, Sprint will also provide Customer with the relevant connector for download together with installation instructions to enable granular administration and reporting for Web Filtering (per Internet user or group).

(B) Sprint reserves the right to modify and update the features and functionality of the Services, at no additional cost to Customer, with the objective of providing Customer with equal or enhanced Services. These updates will include any subsequent release or version of the Services containing functional enhancements, extensions, error corrections or fixes which are generally made available free of charge to Sprint customers who have contracted for the appropriate level of Services. Updates will not include any release, option or future product which Sprint licenses separately or which is not included under the applicable level of support.

(C) Sprint will give Customer prior written notice of any material modification or update, and will seek to ensure that any modifications or updates do not materially degrade the performance of the Services or Customer's use of the Services, or require Customer to incur any additional cost to continue using the Services. Sprint will use reasonable efforts to implement all such modifications or updates in a manner that minimizes the impact on Customer's use of the Services.

3. SERVICE LEVEL AGREEMENT ("SLA").

3.1. Sprint's network will process and deliver Customer's Web requests at least 99.99% of the total hours during every month Customer uses the Services ("Availability"). Availability will be determined on an aggregate basis across all locations for which Customer has ordered Services ("Sites").

3.2. Sprint will provide Customer with both primary and secondary proxy addresses for each Site to which Web traffic for each such Site may be directed. As a result, non-Availability occurs only where Web content sent from a Site to both proxy addresses is not being received, scanned, analyzed, filtered, or transmitted after filtering to end users at the affected Site.

3.3. If Customer believes that Sprint has not met the above SLA, Customer must contact Sprint in writing within 15 business days of the end of the month in which Customer believes the SLA was not met.

3.4. If Sprint fails to meet the Availability commitment, Sprint will provide a credit on Customer's monthly Services fee as follows:

Monthly Service Availability	Performance Credit - % credit of monthly Service fee for Services provided
99.99 – 99.5%	10
99.49 – 99.0%	20
98.99 – 98.5%	30
98.49 – 98.0%	40
97.99 – 97.5%	50
97.49 – 97.0%	60
96.99 – 96.5%	70
96.49 – 96.0%	80
95.99 – 95.5%	90
Below 95.5%	100

3.5. The remedy set out in this section will only be available if Customer has fulfilled all of its obligations under this Annex, the Standard Terms and Conditions and the Agreement and will be Customer's sole and exclusive remedy in contract, tort or otherwise in respect of Non-Availability.

3.6. Sprint will implement, maintain and use appropriate processes, procedures and tools to monitor, calculate and report on the performance of the Services against the service levels set forth in this section. If a dispute arises about Availability, Sprint will make a determination in good faith based on Sprint system logs, monitoring reports and configuration records.

3.7. The Monthly Service Availability SLAs set out in this section do not apply to scheduled maintenance. Sprint does not warrant that the Services will be uninterrupted or error-free.

SprintSecure^{sm} Web Protection
Product Annex

Exhibit 1

WEB AND EMAIL SECURITY SERVICES - ACCEPTABLE USE POLICY

The Customer is responsible for ensuring that all users of the Web and Email Security services (the "Services") are aware of this policy. The Customer is also responsible for ensuring that these regulations are complied with at all times, and shall indemnify Sprint and its suppliers against liability, whether civil or criminal, for any violation by such users as the Customer permit to use the Services.

Users must not under any circumstances whatsoever commit, or attempt to commit, nor aid or abet any action that may threaten the Services, whether deliberate, negligently or innocently – this shall include but is not limited to:

- using the Services for any unlawful, invasive, infringing, defamatory, or fraudulent purpose;
- intentionally sending any virus, worm, Trojan horse or harmful code or attachment with the Services;
- interfering with the use of the Services by other authorized users;
- altering, tampering with or circumventing any aspect of the Services;
- any attempt to crash a Services host or network;
- "denial of service" attacks, or "flooding" attacks against a Services host or network;
- using the Services to send unsolicited bulk commercial email of any kind, regardless of the content or nature of such messages;
- reselling, passing-through, renting, leasing, timesharing or branding the Services or otherwise providing the Services to any party which is not contractually authorized by Sprint to receive the Services;
- testing or reverse-engineering the Services in order to find limitations, vulnerabilities or evade filtering capabilities;
- supplying proprietary information about the Services, including but not limited to screen shots, product documentation, demonstrations, service descriptions, announcements, or feature roadmaps to unauthorized third parties;
- using the Services in a manner not authorized, including use of any features that filter electronic messages for users where a MessageCenter Account has not been established (except as may be permitted in writing by Sprint);
- any attempt to circumvent the user authentication or security of a Services host or network;
- any profligate use of the Services;
- the creation, transmission, storage, or publication of any kind of virus or corrupting program or corrupted data;
- any other action that may adversely affect the Services or their operation.

Sprint shall have the right to suspend or terminate the Services, and to take such defensive action as may at Sprint's sole discretion be deemed necessary in the event of any attack upon the Services or network. Furthermore, Sprint may instigate civil and/or criminal proceedings as appropriate against the perpetrators of such prohibited action.